Transform Set Configuration

This chapter describes how to configure IPSec transform sets.

A transform set is a combination of individual IPSec transforms designed to enact a specific security policy for traffic. During the ISAKMP IPSec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow. Transform sets combine the following IPSec factors:

- Mechanism for payload authentication—AH transform
- Mechanism for payload encryption—ESP transform
- IPSec mode (transport versus tunnel)

A transform set is a combination of an AH transform, plus an ESP transform, plus the IPSec mode (either tunnel or transport mode).

The following topics are discussed:

Process Overview

The basic sequence of actions required to configure an IPSec transform set is outlined below.

Step 1 Configure a crypto transform set by applying the example configuration in Configuring a Transform Set, on page 2.

Step 2 Verify your Crypto Transform Set configuration by following the steps in Verifying the Crypto Transform Set Configuration, on page 2.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring a Transform Set

Use the following example to create the crypto transform set:

```
configure
   context ctxt_name
      crypto ipsec transform-set transform_name ah hmac { md5-96 | none
|sha1-96 } esp hmac { { md5-96 | none | sha1-96 } { cipher {des-cbc |
3des-cbc | aes-cbc } | none }
        mode { transport | tunnel }
        end
```

Notes:

- *ctxt_name* is the system context in which you wish to create and configure the crypto transform set(s).
- *transform_name* is the name of the crypto transform set in the current context that you want to configure for IPSec configuration.
- For more information on parameters, refer to the *IPSec Transform Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Verifying the Crypto Transform Set Configuration

Enter the following Exec mode command for the appropriate context to display and verify your crypto transform set configuration:

```
show crypto ipsec transform-set transform_name
```

This command produces an output similar to that displayed below using the configuration of a transform set named test1.

```
Transform-Set test1 :
AH  : none
ESP : hmac md5-96, 3des-cbc
Encaps Mode : TUNNEL
```